Ethical Hacking

Adarsh Upadhyay[1],Surabhi Patwal[2],Shobhit Kumar[3]
Ccsit,Tmu,Moradabad

[1]Adarshupadhyay168@gmail.com
[2]Surabhipatwal1@gmail.com
[3]Shobhit.computers@tmu.ac.in

Abstract-**The explosive growth of the Internet has brought many good things such as E-commerce-banking, E-mail, Cloud Computing, but there is also a Dark side such as Hacking, Backdoors etc. Hacking is the first big problem faced by Governments, companies, and private citizens around the world , Hacking includes reading others e-mail, steal their credit card number from an on-line shopping site, secretly transmitting secrets to the open Internet. An Ethical Hacker can help the people who are suffered by this Hackings. This Paper Describes about Ethical Hackers, Their Skills, Their Attitudes, and How They Go About Helping Their Customers Find and Plug up Security Holes.**

Keywords:

- Definition
- Types of hackers
- Types of hacking
- Advantage of hacking
- Disadvantage of hacking
- Purpose of hacking
- Techniques of hacking
- Sniffing
- Teminology
- Conclusion
- References

I. INTRODUCTION

An ethical hacker (also known as a whit hacker) is the ultimate security professional. E hackers know how to find and exploit vulnerabi and weaknesses in various systems—just like a malicious hacker (or a black hat hacker).

Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering into them. Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.

Hacking is usually legal as long as it is being done to find weaknesses in a computer or network system for testing purpose. This sort of hacking is what we call **Ethical Hacking**.

Types of Hackers:

1. *Whitehat Hackers:* These are the individuals that perform ethical hacking to help secure companies and organizations. Their belief is that you must examine your network in the same manner as a criminal hacker to better understand its vulnerabilities. A white hacker does it with no criminal intent in mind. Companies around the world, who want to test their systems, contract white hackers.

*2. SCRIPT KIDDIES***:** Script kiddie is a pejorative term for a computer intruder with little or no skill; a person who simply follows directions or uses a cookbook approach — typically using other people's scripts and shellcodes — without fully understanding the meaning of the steps they are performing.

3. *CRACKERS*: Those who will enter your computer just for the fun of it, or prove their technical skills.

4. *Gray-hat Hackers:*

These individuals typically follow the law but sometimes venture over to the darker side of blackhat hacking. It would be unethical to employ these individuals to perform security duties for your organization as you are never quite clear where they stand.

5. black hat Hacker

A black hat hacker, also known as a cracker or a dark side hacker. He uses his skills with a criminal intent. Some examples are: cracking bank accounts in order to make transference to their own accounts, stealing information to be sold in the black market, or attacking the computer network of an organization for money.

Types of Hacking:

a) *Website Hacking* − Hacking a website means taking unauthorized control over a web server and its associated software such as databases and other interfaces.

b) *Network Hacking* − Hacking a network means gathering information about a network by using tools like Telnet, NS lookup, Ping, Tracert, Netstat, etc. with the intent to harm the network system and hamper its operation.

c) Email Hacking − It includes getting unauthorized access on an Email account and using it without taking the consent of its owner.

d) *Ethical Hacking* − Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.

e) *Password Hacking* − This is the process of recovering secret passwords from data that has been stored in or transmitted by a computer system.

f) *Computer Hacking* − This is the process of stealing computer ID and password by applying hacking methods and getting unauthorized access to a computer system.

Advantages of Hacking

- To recover lost information, especially in case you lost your password.
- To perform penetration testing to strengthen computer and network security.
- To put adequate preventative measures in place to prevent security breaches.
- To have a computer system that prevents malicious hackers from gaining access.

Disadvantages of Hacking:

- Massive security breach.
- Unauthorized system access on private information.
- Privacy violation.
- Hampering system operation.
- Denial of service attacks.
- Malicious attack on the system.

Purpose of Hacking:

- Just for fun
- Show-off
- Steal important information
- Damaging the system
- Hampering privacy
- Money extortion
- System security testing
- To break policy break.

Teminolgy:

- *Adware* − Adware is software designed to force pre-chosen ads to display on your system.
- *Attack* − An attack is an action that is done on a system to get its access and extract sensitive data.
- *Back door* − A back door, or trap door, is a hidden entry to a computing device or software that bypasses security measures, such as logins and password protections.
- *Bot* − A bot is a program that automates an action so that it can be done repeatedly at a much higher rate for a more sustained period than a human operator could do it. For example, sending HTTP, FTP or Telnet at a higher rate or calling script to create objects at a higher rate.
- Clone*phishing* − Clone phishing is the modification of an existing, legitimate email with a false link to trick the recipient into providing personal information.
- *Cracker* − A cracker is one who modifies the software to access the features which are considered undesirable by the person cracking the software, especially copy protection features.
- *Denial of service attack* **(DoS)** − A denial of service (DoS) attack is a malicious attempt.
- *DDoS* − Distributed denial of service attack.
- *Firewall* − A firewall is a filter designed to keep unwanted intruders outside a computer system or network while allowing safe communication between systems and users on the inside of the firewall.
- *Malware* −Malware is an umbrella term used to refer to a variety of forms of hostile or intrusive software, including computer viruses, worms, Trojan horses, ransomware, spyware, adware, scareware, and other malicious programs.
- *Master Program* − A master program is the program a black hat hacker uses to remotely transmit commands to infected zombie drones, normally to carry out Denial of Service attacks or spam attacks.
- *Phishing* − Phishing is an e-mail fraud method in which the perpetrator sends out legitimate-looking emails, in an attempt to gather personal and financial information from recipients.
- *Rootkit* − Rootkit is a stealthy type of software, typically malicious, designed to hide the existence of certain processes or programs from normal methods of detection and enable continued privileged access to a computer.
- *Social engineering* − Social engineering implies deceiving someone with the purpose of acquiring sensitive and personal information, like credit card details or user names and passwords.
- *Spam* − A Spam is simply an unsolicited email, also known as junk email, sent to a large number of recipients without their consent.
- *Spoofing* − Spoofing is a technique used to gain unauthorized access to computers, whereby the intruder sends messages to a computer with an IP address indicating that the message is coming from a trusted host.
- *Spyware* − Spyware is software that aims to gather information about a person or organization without their knowledge and that may send such information to another entity without the consumer's consent, or that

asserts control over a computer without the consumer's knowledge.

- *SQL Injection* − SQL injection is an SQL code injection technique, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution (e.g. to dump the database contents to the attacker).
- *Threat* − A threat is a possible danger that can exploit an existing bug or vulnerability to compromise the security of a computer or network system.
- *Trojan* − A Trojan, or Trojan Horse, is a malicious program disguised to look like a valid program, making it difficult to distinguish from programs that are supposed to be there designed with an intention to destroy files, alter information, steal passwords or other information.
- *Virus* − A virus is a malicious program or a piece of code which is capable of copying itself and typically has a detrimental effect, such as corrupting the system or destroying data.
- *Vulnerability* − A vulnerability is a weakness which allows a hacker to compromise the security of a computer or network system.
- *Worms* − A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself.

HACKING ETHICAL TECHNIQUES:

- Password guessing and cracking
- Session hijacking
- Session spoofing
- Network traffic sniffing
- Denial of Service attacks
- Exploiting buffer overflow vulnerabilities
- SQL injection

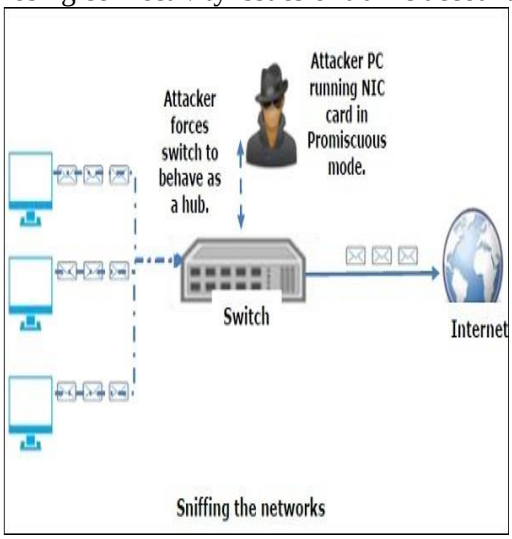
What can be sniffed?

- Email traffic
- FTP passwords
- Web traffics
- Telnet passwords
- Router configuration
- Chat sessions
- DNS traffic

How it works

A sniffer normally turns the NIC of the system to the **promiscuous mode** so that it listens to all the data transmitted on its segment.

Promiscuous mode refers to the unique way of Ethernet hardware, in particular, network interface cards (NICs), that allows an NIC to receive all traffic on the network, even if it is not addressed to this NIC. By default, a NIC ignores all traffic that is not addressed to it, which is done by comparing the destination address of the Ethernet packet with the hardware address (a.k.a. MAC) of the device. While this makes perfect sense for networking, non-promiscuous mode makes it difficult to use network monitoring and analysis software for diagnosing connectivity issues or traffic accounting.



A sniffer can continuously monitor all the traffic to a computer through the NIC by decoding the information encapsulated in the data packets.

Types of Sniffing:

Passive Sniffing-

In passive sniffing, the traffic is locked but it is not altered in any way. Passive sniffing allows listening only. It works with Hub devices. On a hub device, the traffic is sent to all the ports. In a network that uses hubs to connect systems, all hosts on the network can see the traffic. Therefore, an attacker can easily capture traffic going through.

The good news is that hubs are almost obsolete nowadays. Most modern networks use switches. Hence, passive sniffing is no more effective.

Active Sniffing:-

In active sniffing, the traffic is not only locked and monitored, but it may also be altered in some way as determined by the attack. Active sniffing is used to sniff a switch-based network. It involves injecting **address resolution**

packets (ARP) into a target network to flood on the switch **content addressable memory** (CAM) table. CAM keeps track of which host is connected to which port.

Following are the Active Sniffing Techniques −

- MAC Flooding
- DHCP Attacks
- DNS Poisoning

CONCLUSION

"Ethical hacking" seems to be a new buzz word although the techniques and ideas of testing security by attacking an installation aren't new at all. Administrators tested their systems already decades ago and even discussed their ideas and findings in public16. Nevertheless, ethical hacking provides results which can be used to strengthen a information technology environments security nearly immediately. The revealed vulnerabilities and problems may lead to a successful compromise of one or multiple systems – ethical hacking provides data which is based on real tests, which have been successful after all. Problems detected by an ethical hack are for real and should be treated in such a way – fixing the security holes is required. An ethical hack per se doesn't fix or improve the security at all – it does provide information about what should be fixed.

References

[1] Twincling Society Ethical Hacking Seminar. 2006. RetrievedMarch272009.
[2] Krutz, Ronald L. and Vines, Russell Dean. The CEH Prep Guide: T Comprehensive Guide to Certified Ethical Hacking. PublishedJohnWiley and Sons, 2007.
[3] Palmer, Charles. Ethical Hacking. Published in IBM Systems Journal: End-to-End Security, Volume 40, Issue 3, 2001.
[4] Tiller, James S. The ethical hack: a framework for business value penetration testing. Published by CRC Press, 2005.
[5] Beaver, Kevin and McClure, Stuart. Hacking For Dummies. Published by For Dummies, 2006.
[6] Certified Ethical Hacking Seminar. 2006. Retrieved March 27, 2009.
[7] Certified Ethical Hacking EC-Council. 2009. Retrieved March 27, 2009.
[8] Certified Ethical Hacking EC-Council. 2009. Retrieved March 27, 2009.
[9] Ethical Hacking Jobs. 2009. Retrieved March 27, 2009.D'Ottavi, Alberto. Interview: Father of the Firewall. 2003. Retrieved March 27, 2009.